EXHIBIT D

FORENSIC INSPECTION PROTOCOL AGREEMENT

CesiumAstro Inc. ("**Cesium**") and Erik Luther ("**Luther**"), collectively, the "Parties," jointly agree to this Forensic Inspection Protocol Agreement (the "**Protocol**"), which establishes the terms for the imaging, searching and inspection of the Materials (defined below).

TransPerfect Legal Solutions shall serve as the computer forensic examiner ("Forensic Examiner") in this forensic inspection. The Forensic Examiner has been engaged by Cesium to execute the directives contained within this Protocol. However, by entering into this Protocol, neither Party waives the right to seek other, further forensic examination of relevant documents and information through discovery in any future proceeding (and/or by further voluntary agreement of the Parties), and each Party specifically reserves the right to do so. Moreover, nothing in this Agreement waives any claims, objections and/or defenses of the Parties and all such rights and defenses are expressly reserved.

1. Collection of the Materials

Luther, by and through his counsel, shall make available for forensic inspection to the Forensic Examiner the following Materials within three (3) business days of execution of this Protocol.

The Materials are defined as follows:

a. The "two USB flash drives" referenced in the email forwarded from Collin K. Brodrick to Michael P. Royal on Monday, October 16, 2023, at 1:08 PM;

b. The "external hard drive with video files CesiumAstro was planning to use for a public-facing video and a flash drive with three files he had to print at Office Depot," as referenced in the email forwarded from Collin K. Brodrick to Michael P. Royal on Monday, October 16, 2023, at 1:08 PM;

c. Email account: Eluther22@hotmail.com

d. Email account: trudant@hotmail.com

e. Email account: hluther07@icloud.com

The Materials will be provided by Luther, by and through his counsel, to the Forensic Examiner with an accompanying chain of custody, if that chain of custody documentation exists. Luther, by and through his counsel, will provide the Forensic Examiner with usernames, passwords, two-factor authentication, applicable encryption keys, and/or other information needed to allow complete access by the Forensic Examiner.

The Materials and associated usernames, passwords, two-factor authentication, and/or other information needed to allow complete access by the Forensic Examiner shall be provided to the Forensic Examiner within three (3) business days of the execution of this Protocol. While in possession of the Materials, the Forensic Examiner shall retain and maintain the Materials in a secure, confidential environment and limit access to the Materials to staff assigned to work on this case assignment under this Protocol.

2. Preparation for Inspection

As part of the imaging and collection process, the Forensic Examiner shall take all necessary digital photographs and shall record the specifications, characteristics, serial numbers (physical and volume), along with the current physical condition and operability. Prior to imaging, the Forensic Examiner shall properly prepare suitable forensic storage media ("**Target Media**") for receipt of any forensic images created through the Forensic Examiner's execution of any directives under this Protocol.

3. Collection and Remediation of USB devices and External Hard Drive:

The Forensic Examiner will utilize industry-standard forensic tools make a complete and forensically-sound collection of the storage devices.

The Forensic Examiner will preserve the collected data on a set of redundant, encrypted hard drives to prevent unintended access to custodian data and to prevent catastrophic data loss. The collected data will be stored offline in the forensic laboratory's secure evidence vault. Access to such vaults is restricted to Transperfect forensic personnel, and the vaults are secured behind three layers of keycard/PIN access. The evidence vault is located at the Transperfect Forensic Lab 1717 Main Street, Suite 3950, Dallas, Texas, 75201.

When data is requested by Client or Outside counsel to be exported for review, TLS will access one of the redundant encrypted hard drives:

a. The Forensic Examiner will parse the forensic image using a forensic tool.
b. Prior to the Forensic Examiner conducting any forensic analysis/examination (a "**Review**") of any forensic image created from the Materials, the Forensic Examiner shall ensure that all partitions are displayed/recovered and shall then execute the EnCase "Recover Folders" command (or similar command if using another forensic software tool), and shall save the results of the same for inclusion within the Review. The Forensic Examiner shall also include in the Review the "volume shadow copies" and the "Lost Files" category of documents, as defined by the Encase software documentation (or similar functionality if using another forensic software tool).
c. The Forensic Examiner will then ensure that all container files have been fully traversed and that all files, metadata and their contents are searchable. This would include, but is not limited to, technologies such as optical character recognition of all images and non-searchable PDF documents.
d. The Forensic Examiner will export/convert the requested data set(s) into a format that can be ingested to a Review Platform.

e. Counsel will identify items to be remediated and provide list to the Forensic Examiner. See Paragraph 7 below.
f. The Forensic Examiner will delete identified files and then overwrite the slack space on the devices with zeros.
g. The Forensic Examiner will re-image the devices post-remediation and inspect to ensure all identified items have been removed.
h. After the Materials identified in paragraphs 1(a) and 1(b) have been forensically imaged, the Forensic Examiner will securely store them at its premises until execution of the remediation and return procedures in Paragraph 7 below.

The Forensic Examiner shall document and record on an acquisition form: (i) a general description of the process and tools utilized to conduct the collection; (ii) the MD5 hash value of the original source of such Materials; and (iii) the MD5 hash value of the copy.

4. Collection and Remediation of Email Accounts:

a. Counsel will provide the Forensic Examiner with credentials to the email accounts. Assistance with two-factor authentication may be needed from the custodian.
b. The Forensic Examiner will disable user access to the accounts.
c. The Forensic Examiner will utilize industry-standard forensic tools to make a complete and forensically-sound collection of the email accounts.
d. The Forensic Examiner will preserve the collected data on a set of redundant, encrypted hard drives to prevent unintended access to custodian data and to prevent catastrophic data loss. The collected data will be stored offline in the forensic laboratory's secure evidence vault. Access to such vaults is restricted to Transperfect forensic personnel, and the vaults are secured behind three layers of keycard/PIN access. The evidence vault is located at the Transperfect Forensic Lab 1717 Main Street, Suite 3950, Dallas, Texas, 75201.
e. The Forensic Examiner will export the requested data set(s) into an .eml or .pst format for ingestion into a Review Platform.
f. Counsel will identify items to be remediated and provide list to the Forensic Examiner. See Paragraph 7 below.
g. The Forensic Examiner will remove the items, empty the deleted items folder, and remove the items from the "Recoverable items" folder.
h. The Forensic Examiner will re-collect the email accounts post-remediation and inspect to ensure all identified items have been removed.

5. Search for Data

For the Materials identified in Paragraphs 1(a), 1(b), 1(c) and 1(d) above, the Forensic Examiner shall conduct a search of the Materials for information that are hits to the following Data Search Terms: (i) "@cesiumastro.com" (ii) "cesium" (iii) "astro" (iv) "SDR," (v) "RF,"

(vi) "radio," (vii) "frequency," (viii) "signal," and otherwise comply with the following steps in this Protocol. The Forensic Examiner shall use and apply the Data Search Terms to the Materials identified in Paragraphs 1(a), 1(b), 1(c) and 1(d) above and determine if there are any responsive "hits" in documents, files, file names, and/or folder names in such Materials. Any "Hits" on Materials created before February 10, 2021, shall be excluded from this review and not provided to counsel for Cesium.

6. Reporting Requirements

The Forensic Examiner shall record in a log (the "**Hit Log**"), any items, files, folder names, and/or file names that were responsive to the Data Search Terms. Each entry in the Hit Log shall contain the responsive search term and a unique item reference number, e-mail/chat metadata (to, from, cc, bcc, subject, attachment/names, date sent, date received), File Name, File Signature, File Size, MD5 hash value, file metadata including the dates and times for File Created, Last Written, File Description (archive, file, folder, overwritten, deleted, etc.) Last Accessed, Entry Modified, date added and Full Path values.

After the Forensic Examiner has completed the tasks set forth in Paragraph 5, the Forensic Examiner shall create a forensically sound image of all "Hits" and provide a copy of same to counsel for Cesium and counsel for Luther, except as provided in the next sentence. The Forensic Examiner shall create a separate forensically sound image of all "Hits" that also include any of the following terms: "@ogletree.com," "@ogletreedeakins.com," "@jeffreygoldberglaw.com," and/or "@fultonjeang.com," and provide a copy of same ONLY to counsel for Luther. Counsel for Luther shall review these "Hits," determine whether any of the "Hits" contain privileged communications, and if so, list them on a privilege log. Any "Hits" on materials generated before February 10, 2021 need not be logged. If the "Hits" do not contain any privileged information or the privileged communication can be redacted (leaving only unprivileged communications/information), then counsel for Luther shall work with the Forensic Examiner to make same available to counsel for Cesium. The Forensic Examiner shall likewise maintain one copy of the forensic images of all such "hits."

All of the "Hits" provided to Counsel for Cesium and for Luther shall be designated in the following manner under the Confidentiality Agreement, which will be executed at the same time as this Protocol:

- The "Hits" from the Materials identified in Paragraphs 1(a) and 1(b) shall be designated as Attorney Eyes Only;

- For the Materials identified in Paragraphs 1(c), 1(d), and 1(e), any "Hits" generated by the term @cesiumastro.com shall be designated as Confidential; and

- The remaining "Hits" from the Materials identified in Paragraphs 1(c), 1(d), and 1(e) shall be designated as Attorney Eyes Only.

After counsel for the Parties complete their respective review of the "hits," they shall meet and confer in good faith to determine whether the confidentiality designation of any

"Hits" should be modified from Attorney Eyes Only to only Confidential, *i.e.*, because such document/information may contain Cesium's business information, which may be subject to return to and review by Cesium.

7. Remediation and Return of Materials

Cesium's counsel and Luther's counsel will confer in good faith to identify which, if any, of the data on the Materials constitute Cesium business information or property. Once an agreement is reached, counsel for the Parties shall jointly draft and transmit to the Forensic Examiner a list of the files to be permanently deleted. The Forensic Examiner will confirm to Cesium's counsel and Luther's counsel in writing once the deletion is completed. The Forensic Examiner will return the physical Materials to Luther within one (1) business day of completing the deletion and re-enable custodian access to the email accounts. The Forensic Examiner will retain and maintain the confidentiality of all copies of the forensic images and all other data extracted from the Materials after returning the Materials to counsel Luther, unless jointly instructed otherwise by counsel for both Parties and/or by an order of a court of competent jurisdiction.

8. No Waiver of Privilege and No Waiver of Rights and Defenses; Confidential Treatment of Materials

The Parties agree that the analysis to be conducted by the Forensic Examiner under this Protocol does not constitute a waiver of any privilege. Nor does the Parties' agreement to proceed with the forensic examination contemplated by this Protocol constitute an admission of liability, or a waiver of any defense, including a defense to disclosure of documents and information, in these proceedings.

All reports, disclosures, documents and information contemplated by or referenced in this Protocol shall not be disclosed by the Forensic Examiner to any third party, except where the Parties may otherwise mutually provide or designate (or a Court orders) in the future.

9. Cooperation

The Parties agree to cooperate in good faith with one another to complete all tasks set forth in this Protocol and to do their best to proceed quickly through all of the steps.

10. Third Party Inquiries

If the Forensic Examiner is served with a subpoena or court order, which appears valid on its face and which seeks some or all of the Materials (and/or any images, documents or Reports generated under this Protocol), the Forensic Examiner shall promptly inform the Parties of such subpoena or order. The Party whose information is the subject of the subpoena or order shall thereafter be responsible for preparing such objections and/or preparing and filing such motions or applications to limit or prevent disclosure of such information.

11. Reservation of Right to Recover Fees and Costs

All of the costs and expenses invoiced by the Forensic Examiner in connection with this Protocol shall be borne solely by Cesium.

/s/ Donald W. Myers
Counsel for and on behalf of Cesium

/s/ *Collin K. Brodrick*
Counsel for and on behalf of Luther

WHR
Corporate representative of Cesium

DocuSigned by:
Erik Luther
4CE89B5F6D374A1...
Erik Luther

Title: Chief of Staff